

## AUTOMORPHISMS OF SMALL PRIME POWER GROUPS

JOSHUA MAGLIONE

ABSTRACT. If  $f(p, n)$  is the number of pairwise nonisomorphic groups of order  $p^n$ , and  $g(p, n)$  is the number of groups of order  $p^n$  whose automorphism group is a  $p$ -group, then, for  $n \leq 7$ , we prove that the ratio  $g(p, n)/f(p, n)$  is bounded away from 1 as the prime  $p$  grows to infinity. In addition, we provide some data on the number of groups whose automorphism group is a group of prime power order, for primes no larger than 11.

## 1. INTRODUCTION

Within the last decade, we have gained incredible knowledge about the automorphism groups of  $p$ -groups. Nevertheless, we are still unable to answer basic questions like the following found in [M2]. If  $f(p, n)$  is the number of pairwise nonisomorphic groups of order  $p^n$  and  $g(p, n)$  the number of groups of order  $p^n$  whose automorphism group is a  $p$ -group, then does

$$(1) \quad \lim_{n \rightarrow \infty} \frac{g(p, n)}{f(p, n)} = 1?$$

A recent result of Martin and Helleloid-Martin is summarized as follows. The automorphism group of almost all  $p$ -groups is a  $p$ -group [HM, Theorem 1]. However, Helleloid-Martin's perspective differs from the perspective of Mann's question in (1). Instead, they consider three parameters: the prime, the number of generators, and the  $p$ -class. They prove three limits by fixing two parameters and allowing one to vary, and they provide a list of boundary conditions for which their theorem need not hold. Here, we verify, in some sense, the necessity of some of those boundary conditions with the following theorem.

**Theorem 1.** *Let  $f(p, n)$  be the number of pairwise nonisomorphic groups of order  $p^n$  and  $g(p, n)$  the number of groups of order  $p^n$  whose automorphism group is a  $p$ -group. If  $n \leq 7$ , then*

$$\lim_{p \rightarrow \infty} \frac{g(p, n)}{f(p, n)} \leq \frac{2}{3}.$$

A sharper upper bound likely exists — certainly, for individual  $n$  values. The interest is not in the limit itself, but in the fact that this limit is bounded away from 1. Thus, we do not get a statement like that of Helleloid-Martin for small  $p$ -groups. In fact, it may be that the majority of these automorphism groups are not  $p$ -groups.

In addition to Theorem 1, we provide data on the number of automorphism groups of various small  $p$ -groups for  $p \leq 11$ , which expands on the known values,  $p \leq 5$  and  $n \leq 7$ , as seen in [HM, p. 295]. In order to make the computation quicker, we use techniques described in [W, M] to find more characteristic subgroups outside

of the standard verbal and marginal ones. For the majority of these groups, we find many more characteristic subgroups. In order to carry out these computations for groups of order  $11^7$ , we use ideas in [BMW]. Indeed, the groups of genus 1 and 2 are still quite an obstacle; some of whose automorphism group requires several hours to compute in MAGMA V2.21-1 on an Intel Xeon W3565 at 3.20 GHz. These tables require about 8 months of computation even with the state of the art algorithms.

## 2. PRELIMINARIES

**2.1. Notation.** We denote the set of nonnegative integers by  $\mathbb{N}$ , and the set of all subsets of a set  $G$  by  $2^G$ . For groups and rings, we follow standard notation found in [G]. For  $g, h \in G$ , we set

$$[g, h] = g^{-1}g^h = g^{-1}h^{-1}gh;$$

for  $X, Y \subseteq G$ , we set

$$[X, Y] = \langle [x, y] : x \in X, y \in Y \rangle.$$

We let  $\mathbb{Z}_p$  denote the group  $\mathbb{Z}/p\mathbb{Z}$ .

For a  $p$ -group  $G$ , the lower central series of  $G$  is defined recursively with  $\gamma_1(G) = G$  and  $\gamma_{i+1}(G) = [\gamma_i(G), G]$ . Similarly, the exponent  $p$ -central series of  $G$  is defined by  $\eta_1(G) = G$ , and  $\eta_{i+1}(G) = [\eta_i(G), G]\eta_i(G)^p$ . If  $\gamma_c(G) \neq 1$  and  $\gamma_{c+1}(G) = 1$ , then  $G$  has (nilpotency) *class*  $c$ . Similarly, if  $\eta_c(G) \neq 1$  and  $\eta_{c+1}(G) = 1$ , then  $G$  has  *$p$ -class*  $c$ . Suppose  $P$  and  $G$  are  $p$ -groups with  $p$ -class  $c$  and  $c+1$  respectively. We say  $G$  is an *immediate descendant* of  $P$  if  $G/\eta_{c+1}(G) \cong P$ . If  $G$  is  $p$ -class 2, of order  $p^n$ , and  $\log_p[G : \Phi(G)] = d$ , then, for our purposes, we say the *genus* of  $G$  is  $n - d$ . A more general definition of genus in the context of groups is described in [BMW].

**2.2. Filters.** We use filters to gain exponential improvements in computing the automorphism groups of some small  $p$ -groups. In [W], J. B. Wilson introduced filters as a generalization of an  $N$ -series, defined by Lazard in [L]. The appeal of filters is to have access to an associated graded Lie ring, and hence, they are easy to compute with on account of capturing linear structure.

**Definition 2.** Let  $\langle M, 0, +, \preceq \rangle$  be a commutative monoid with pre-order, and  $G$  a group. A filter is a function  $\phi$  from  $M$  into the subgroups of  $G$  satisfying the following conditions for all  $s, t \in M$ :

- (1)  $[\phi_s, \phi_t] \leq \phi_{s+t}$ , and
- (2)  $s \preceq t$  implies  $\phi_s \geq \phi_t$ .

Every filter  $\phi : M \rightarrow 2^G$  induces a *boundary filter*  $\partial\phi : M \rightarrow 2^G$  where  $\partial\phi_s = \langle \phi_{s+t} | t \in M - \{0\} \rangle$ . With this, we can define a graded Lie ring for  $G$ . Define  $L(\phi) = \bigoplus_{s \in M} \phi_s / \partial\phi_s$ , where  $L_0 = 0$ , with multiplication given by

$$[\partial\phi_s x, \partial\phi_t y] = \partial\phi_{s+t}[x, y].$$

**Theorem 2** ([W, Theorem 3.1]).  *$L(\phi)$  is an  $M$ -graded Lie ring.*

As the filter refines so does its associated Lie ring. Our aim is to construct long characteristic series with an associated graded Lie algebra. We assume our monoids are  $\mathbb{N}^d$  for some  $d$ . Provided we can find a new characteristic subgroup to add to our filter, we can use this new subgroup to generate more characteristic subgroups throughout the filter. Indeed, suppose  $\pi : X \rightarrow 2^G$  satisfies

- (1)  $0 \in X \subseteq \mathbb{N}^d$  and  $\langle X \rangle = \mathbb{N}^d$ ;
- (2) if  $s \in X$  and  $t \in \mathbb{N}^d$  with  $t \preceq s$ , then  $t \in X$ ;
- (3) for all  $s \in X$ ,  $\pi_s \preceq G$ ;
- (4) if  $s, t \in X$  with  $s \preceq t$ , then  $\pi_s \geq \pi_t$ .

For  $s \in \langle X \rangle$ , a *partition* of  $s$  with respect to  $X$  is a sequence  $(P_1, \dots, P_k)$  where each  $P_i \in X$  and  $s = \sum_{i=1}^k P_i$ . Let  $\mathcal{P}_X(s)$  denote the set of partitions of  $s \in \langle X \rangle$  with respect to  $X$ , and if  $P = (P_1, \dots, P_k) \in \mathcal{P}_X(s)$ , then set

$$[\pi_P] = [\pi_{P_1}, \dots, \pi_{P_k}].$$

We generate a filter  $\bar{\pi} : \langle X \rangle \rightarrow 2^G$  defined as follows

$$\bar{\pi}_s = \prod_{P \in \mathcal{P}_X(s)} [\pi_P],$$

cf. [W, Theorem 3.3].

We are back to the problem of finding characteristic subgroups in a  $p$ -group. Suppose we start with the filter  $\eta : \mathbb{N} \rightarrow 2^G$  given by the exponent  $p$ -central series of  $G$ . Then  $L(\eta)$  has an associated  $\mathbb{N}$ -graded Lie algebra, which yields  $\mathbb{Z}_p$ -bilinear maps from the graded product (eg.  $[\cdot, \cdot] : L_s \times L_t \rightarrow L_{s+t}$ ). We turn to some associated algebras for these bilinear maps. Suppose  $\circ : U \times V \rightarrow W$  is a biadditive map of abelian groups; define the adjoint, centroid, and derivation rings as

$$\text{Adj}(\circ) = \{(f, g) \in \text{End}(U) \times \text{End}(V)^{\text{op}} : \forall u \in U, \forall v \in V, uf \circ v = u \circ gv\},$$

$$\begin{aligned} \text{Cent}(\circ) = \{(f, g, h) \in \text{End}(U) \times \text{End}(V) \times \text{End}(W) : \forall u \in U, \forall v \in V, \forall w \in W, \\ uf \circ v = u \circ vg = (u \circ v)h\}, \text{ and} \end{aligned}$$

$$\begin{aligned} \text{Der}(\circ) = \{(f, g, h) \in \mathfrak{gl}(U) \times \mathfrak{gl}(V) \times \mathfrak{gl}(W) : \forall u \in U, \forall v \in V, \forall w \in W, \\ uf \circ v + u \circ vg = (u \circ v)h\}. \end{aligned}$$

It is in these rings we find more characteristic structure in  $G$  [W, Section 4]. Indeed, the Jacobson radical acts on the homogeneous components and yields characteristic subgroups (for  $\text{Der}(\circ)$ , this is done in the associative enveloping algebra).

### 3. DATA

We provide data on the number of  $p$ -groups whose automorphism group is also a  $p$ -group in Tables 1 and 2. We examine the groups of order 512, and for each group, we record the change in length of the filter and the change in order of the largest factor. The longer the filter, or the smaller the largest factor, the faster we can compute the automorphism groups. Our data is found in Figures 1 and 2. Some data on the kinds of refinements which seem most successful can be found in [W2]. All of these computations were done in MAGMA [BCP].

The timing of the algorithm for computing the automorphism group of a  $p$ -group is heavily dependent on the orders of the factors of the characteristic series it works with [O, ELGO]. In fact, the algorithm is exponential in the order of the largest factor. Therefore, Figure 1 is an incomplete picture of how the rings in Section 2 aid in the computation. On the other hand, we see that, in Figure 2, about 80% of groups of order 512 have an exponential speed-up. Thus, without these improvements, the computation of the automorphism groups would be orders of magnitude harder.

Order	$p^5$	$p^6$	$p^7$
$p = 2$	36 of 51	211 of 267	2,067 of 2,328
$p = 3$	0 of 67	30 of 504	2,119 of 9,310
$p = 5$	1 of 77	65 of 674	11,895 of 34,297
$p = 7$	0 of 83	91 of 860	42,208 of 113,147
$p = 11$	1 of 87	189 of 1,192	286,385 of 750,735

TABLE 1. The number of  $p$ -groups whose automorphism group is a  $p$ -group.

Order	$p^8$	$p^9$
$p = 2$	54,463 of 56,092	10,477,331 of 10,494,213
$p = 3$	1,002,258 of 1,396,077	

TABLE 2. The number of 2-groups whose automorphism group is a 2-group.

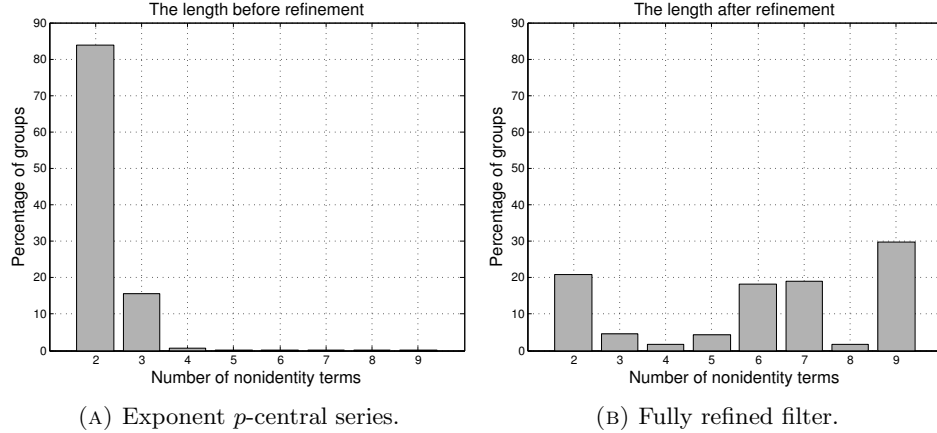


FIGURE 1. The bar graphs show how long a characteristic series gets by refining the  $p$ -central series using  $\text{Adj}(\circ)$ ,  $\text{Cent}(\circ)$ , and  $\text{Der}(\circ)$  for groups of order 512. The maximum possible is 9.

#### 4. PROOF OF THEOREM 1

We prove Theorem 1 by considering the possible values for  $n$ , while assuming  $p$  is an odd prime. The statement of the theorem is immediate for  $n \leq 4$  because, in that case, there is a constant number of groups of order  $p^n$ . For each  $n \leq 4$ , at least one third of the groups of order  $p^n$  are abelian. Thus, for each of those groups, there exists an automorphism which is an involution.

*Proof of Theorem 1.* The theorem follows for  $n \leq 4$ , so we first consider when  $n = 5$ . Suppose  $G$  has order  $p^5$  and  $G' = G^p = Z(G) \cong \mathbb{Z}_p^2$ . There exists generators  $x, y, z$  for  $G$  such that  $G' = \langle [y, x], [z, x] \rangle$  and  $[z, y] = 1$ . In addition, we assume that  $G^p = \langle y^p, z^p \rangle$ . There are at least  $p + O(1)$  such groups [VL, p. 12]. If  $x^p \neq 1$ ,

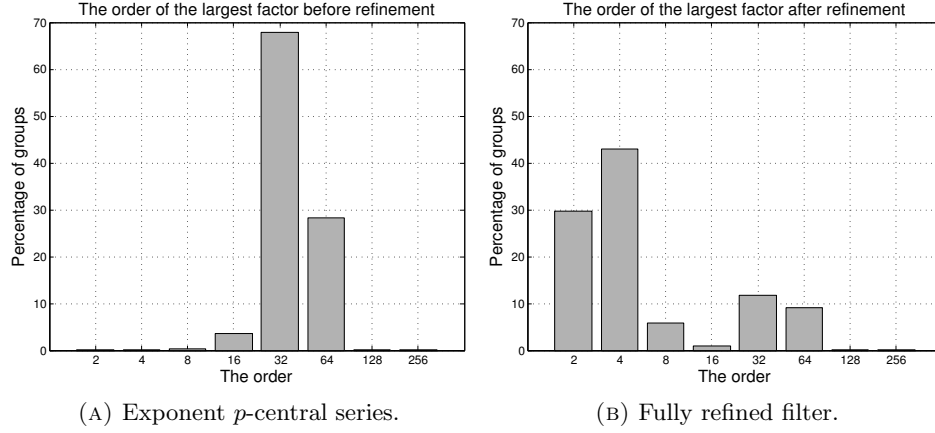


FIGURE 2. The bar graphs show the orders of the largest factors in each of the series for groups of order 512. The larger the sections, the harder it is to compute the automorphism group.

then there exists  $a, b \in \mathbb{Z}_p$  such that  $\bar{x} = xy^a z^b$  and  $\bar{x}^p = 1$  because  $G^p = \langle y^p, z^p \rangle$ . Thus, without loss of generality, we assume  $x^p = 1$ . The map fixing  $x$  and inverting  $y$  and  $z$  induces an automorphism of  $G$ . Since there are  $2p + O(1)$  groups of order  $p^5$ , the theorem follows for  $n = 5$ .

Now suppose  $n = 6$ ,  $p \geq 5$ , and  $G$  is a group of order  $p^6$ , which is an immediate descendant from

$$P = \langle x, y, z \mid [z, x] = [z, y] = 1, \text{class } 2, \text{exponent } p \rangle.$$

Nearly all groups of order  $p^6$  are immediate descendants of  $P$ , but about one third of them satisfy these equations

$$(3) \quad \begin{aligned} [z, x] &= [y, x, x], \\ [z, y] &= [y, x, z] = z^p = 1. \end{aligned}$$

The map which inverts  $x$  and  $y$  and fixes  $z$  induces an automorphism of  $G$ . There are  $p^2 + O(p)$  groups of order  $p^6$  that satisfy (3) [VL2, p. 37], and there are  $3p^2 + O(p)$  groups of order  $p^6$  [NOVL].

Let  $G$  be a group of order  $p^7$  for  $p \geq 5$ , and suppose that  $G$  is an immediate descendant of

$$Q = \langle x, y, z \mid [z, y] = 1, \text{class } 2, \text{exponent } p \rangle.$$

An abundant source of these descendants satisfy these sets of equations, as seen in [OVL2],

$$(4) \quad \begin{aligned} 1 &= [z, y] = [y, x, z], \\ [y, x, x] &= [z, x, z], \\ [z, x, x] &= [y, x, y]. \end{aligned}$$

The map which inverts  $x$ ,  $y$ , and  $z$  induces an automorphism of  $G$ . There are  $p^5 + O(p^4)$  groups that satisfy (4) [OVL2, pp. 56 – 57]. Since there are  $3p^5 + O(p^4)$  groups of order  $p^7$  for  $p \geq 5$ , the theorem follows.  $\square$

Because Helleloid-Martin consider a different ratio from  $g(p, n)/f(p, n)$ , Theorem 1 does not fit nicely into their framework. However, their result is the closest comparison to Theorem 1. In fact, when they fix the number of generators and  $p$ -class but let the prime vary, they do not consider the families of groups in the proof of Theorem 1, and in this light, it seems reasonable to guess that the theorem of Helleloid-Martin might not hold for smaller values than they reported. Therefore, while improvements for the choice of values for the parameters might be possible, we suggest that they are likely close to optimal.

#### ACKNOWLEDGEMENTS

The author is thankful to James B. Wilson and Alexander Hulpke for helpful feedback and to Eamonn A. O'Brien for his initial question.

#### REFERENCES

- [BCP] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265. Computational algebra and number theory (London, 1993). MR1484478
- [BMW] Peter A. Brooksbank, Joshua Maglione, and James B. Wilson, *Isomorphism on the edge of wilderness*, in preparation.
- [ELGO] Bettina Eick, C. R. Leedham-Green, and E. A. O'Brien, *Constructing automorphism groups of  $p$ -groups*, Comm. Algebra **30** (2002), no. 5, 2271–2295. MR1904637 (2003d:20027)
- [G] Daniel Gorenstein, *Finite groups*, 2nd ed., Chelsea Publishing Co., New York, 1980. MR569209 (81b:20002)
- [HM] Geir T. Helleloid and Ursula Martin, *The automorphism group of a finite  $p$ -group is almost always a  $p$ -group*, J. Algebra **312** (2007), no. 1, 294–329. MR2320459 (2008h:20035)
- [L] Michel Lazard, *Sur les groupes nilpotents et les anneaux de Lie*, Ann. Sci. Ecole Norm. Sup. (3) **71** (1954), 101–190 (French). MR0088496 (19,529b)
- [M1] Joshua Maglione, *Longer characteristic series for classical unipotent subgroups*, J. Group Theory, in press.
- [M2] Avinoam Mann, *Some questions about  $p$ -groups*, J. Austral. Math. Soc. Ser. A **67** (1999), no. 3, 356–379. MR1716701 (2000k:20051)
- [NOVL] M. F. Newman, E. A. O'Brien, and M. R. Vaughan-Lee, *Groups and nilpotent Lie rings whose order is the sixth power of a prime*, J. Algebra **278** (2004), no. 1, 383–401. MR2068084 (2005c:20034)
- [O] E. A. O'Brien, *The  $p$ -group generation algorithm*, J. Symbolic Comput. **9** (1990), no. 5-6, 677–698. Computational group theory, Part 1. MR1075431 (91j:20050)
- [OVL1] E. A. O'Brien and M. R. Vaughan-Lee, *The groups with order  $p^7$  for odd prime  $p$* , J. Algebra **292** (2005), no. 1, 243–258. MR2166803 (2006d:20038)
- [OVL2] ———, *Notes on the construction of the groups with order dividing  $p^7$*  (2004), [www.math.auckland.ac.nz/~obrien/research/p7.html](http://www.math.auckland.ac.nz/~obrien/research/p7.html), Accessed March 2015.
- [VL1] Michael Vaughan-Lee, *Nilpotent Lie rings of order  $p^5$*  (2002). Notes.
- [VL2] ———, *Nilpotent Lie rings of order  $p^6$*  (2002). Notes.
- [W1] James B. Wilson, *More characteristic subgroups, Lie rings, and isomorphism tests for  $p$ -groups*, J. Group Theory **16** (2013), no. 6, 875–897. MR3198722
- [W2] ———, *New Lie products for groups and their automorphisms*, in preparation. arXiv:1501.04670.

DEPARTMENT OF MATHEMATICS, COLORADO STATE UNIVERSITY, FORT COLLINS, CO 80523, USA

*E-mail address:* maglione@math.colostate.edu